Available online at www.sciencedirect.com

ScienceDirect

IERI Procedia 4 (2013) 303 – 308

Procedia IERI

www.elsevier.com/locate/procedia

2013 International Conference on Electronic Engineering and Computer Science

A Secure Credit Recharge Scheme for Mobile Payment System in Public Transport

Haowei Su[a,]*, Xiaoli Wen[a], Dabi Zou[a]

[a]*Guangzhou Yangchengtong Co., Ltd, Guangzhou 510080, P.R.China*

Abstract

This paper first studies the emerging requirements of mobile payment system by way of NFC cell phones, etc., in public transport, especially the security challenges. Then, a secure credit recharge scheme is proposed to cover these new requirements. In the proposed scheme, we make use of a shared secret between the smart card and the server to build a mutual authenticated and secret communication path. The paper also analyzes the security aspects of the proposed scheme, and the analysis and practices show the scheme could meet the security requirements of mobile payment in public transport.

Keyword s: Mobile Payment, Smart Card, Security, Mutual Authentication

1. Introduction

With the development of wireless telecommunication and hardware technology, mobile phones are becoming more and more intelligent and powerful. They can be used to do a lot of work which could only be handled by personal computers previously. Among them, mobile payment, with its definition as any transaction with monetary value that is conducted via a mobile telecommunications network[1], is one of

* Corresponding author. Tel.: +86-20-87695121; fax: +86-20-37651820.
E-mail address: gzsuhw@tom.com.

doi:10.1016/j.ieri.2013.11.043

those having huge potential market attractiveness, and it is becoming a hot spot and getting rapid growth both in the community and business in these years, and there is quite a few mobile payment systems proposed[2~8].

Near field communication (NFC) is a set of standards for smart phones and similar devices to establish radio communication with each other by touching them together or bringing them into close proximity, usually no more than a few centimeters. It is a key enabling technology for mobile payment services. Powered with NFC features, smart phones could be used in public transport and financial and several other fields to achieve better mobile payment service experiences.

There are several main hardware solutions to power smart phones with NFC features.

- Embedded Secure Element. NFC radio controller, the secure element and NFC software are all in one chip embedded in the NFC phone. The Google Nexus S is one of such phones.
- SWP with SIM-Card. There is a NFC chip in the NFC phone, using single wire protocol (SWP) for connection with SIM/UICC card. The SIM card is the secure environment. This approach is considered the most popular at the moment, and that seems more favorable for a carrier.
- Secure Element on Micro-SD Card. There is a NFC chip in the phone, and it communicates with micro-SD card. The European Payments Council considers it the quickest way to deploy mobile payment.
- NFC covers. All the NFC features are in the NFC cover specially made for iPhone [10].
- NFC devices using audio port. All the NFC features are in a small device (so called box), and the phone communicate with the box through its audio port [11].

In big cities, a huge number of people travel by public transport every day. At the same time, smart phone is becoming more and more popular among mobile phone users. All these factors make mobile payment could play its key role in public transport. In the payment system, user (public transport card holder) makes use of the mobile application installed in her NFC phone to communicate with the server system online to achieve credit recharge, account balance query, transaction detail query, etc. User could accomplish both online consumption and offline consumption by the NFC phone as well.

In the implementation of phone application, the application has to interact with smart card attached to the NFC phone by sending APDU (application protocol data unit) commands. There is a key security challenge, i.e. how to authenticate a terminal application before authorizing its interactions with the server system run by public transport system operator?

One possible solution is to make use of asymmetric cryptographic algorithms supported by security chips in smart cards. In fact, there is a mobile payment system for merchant micropayments [9], which is built on NFC Cover. In their system, they leverage the PKI application features embedded in NFC cover to provide mutual authentication during payment transactions. Thus this payment system is based on the PKI capability provided by NFC cover. However, due to limited resources and cost consideration, smart card applications in most of the above hardware solutions could not support strong authentication algorithms, e.g. PKI RSA algorithms.

In this paper, we propose a new mutual authentication scheme based on a shared secret between the smart card and the public transport server system, without the need of intensive asymmetric cryptographic computation, and thus is practical for different hardware solutions when implementing mobile payment services. Based on this authentication mechanism, we propose a secure credit recharge scheme for public transport system. Security analysis and practices show that the proposed scheme is both secure and feasible.

2. A Secure Credit Recharge Scheme

The proposed secure credit recharge scheme for public transport system mainly considered in two parts. The first part is a new mutual authentication mechanism. This mechanism is based on a shared secret between the smart card (client) and the system operator server (server). The second part is the proposed secure credit